Ataque de ransomware estimula o maior produtor e reciclador de plásticos da América Latina a aumentar a segurança e obter escalabilidade com a Sophos

CUSTOMER-AT-A-GLANCE

valgroup

Valgroup

Indústria
Indústria Plástica

Soluções Sophos
Sophos Intercept X Advanced com XDR: 2.550 licenças
Sophos Intercept X Advanced com XDR para servidor: 200 licenças
Sophos Email Advanced: 2.850 licenças
Sophos Encryption: 500 licenças
Sophos Central

“Embora não houvesse sinais de exfiltração de dados confidenciais, a diretoria “não poupou esforços.“

Arthur Brandão
Gerente de Infraestrutura, Operações e Segurança da Informação

Desafios

- A solução de segurança existente falhou ao impedir um ataque de ransomware.
- A consequente paralisação operacional causou impacto financeiro negativo para a empresa.
- A equipe de TI estava sobrecarregada de trabalho enquanto lutava para restaurar rapidamente o ambiente.
- As soluções de segurança fragmentadas em diferentes grupos eram ineficientes para gerenciar e careciam de escalabilidade.

Com mais de 40 fábricas em seis países, o Valgroup é um dos maiores transformadores de plástico do mundo. Embora a maioria de suas fábricas esteja localizada em todo o Brasil, a empresa também possui operações de fabricação no Uruguai, México, Estados Unidos, Itália e Espanha. A empresa multinacional produz produtos de embalagem, como garrafas plásticas, filmes, rótulos e outras variedades de aplicações, incluindo bens de consumo embalados, agrícolas, industriais e de varejo. Com 45 anos de história, a empresa agora está voltada para o futuro: seu objetivo é liderar a indústria do plástico em sustentabilidade e metas sociais em benefício de seus 6.500 funcionários e do mundo.

Arthur Brandão, baseado em São Paulo, atua com TI há 20 anos e como Gerente de Infraestrutura, Operações e Segurança da Informação da organização há 2. Uma de suas prioridades no Valgroup é ajudar a empresa a ampliar seus processos de segurança e gerenciamento de segurança à medida que expande suas operações e presença global. Anteriormente, cada grupo da empresa adquiria e gerenciava soluções de segurança de forma independente e local com suas próprias equipes de TI.

"Durante o processo de resposta a incidentes, o Sophos Threat Analysis Center foi um recurso essencial."

Arthur Brandão
Gerente de Infraestrutura, Operações e Segurança da Informação

Quais desafios de segurança um fabricante multinacional enfrenta que levariam à necessidade da Sophos?

Arthur Brandão explicou que muitas das ferramentas de segurança implementadas pelos grupos gerenciados independentemente no Valgroup ofereciam apenas monitoramento limitado. Isso surgiu como um problema real quando uma das empresas do grupo empresarial sofreu um ataque de ransomware, em agosto de 2021, porque a solução de segurança existente não conseguiu identificar e bloquear a ameaça. Com as estações de trabalho e servidores da empresa comprometidos, as operações foram paralisadas para que a equipe de TI pudesse remediar o ataque e restabelecer o ambiente com a maior rapidez e segurança possíveis.

Como um ataque de ransomware afeta uma grande operação de produção?

Arthur Brandão observou que, como produtora de plásticos industriais, a empresa normalmente opera 24 horas por dia, 7 dias por semana. A paralisação das operações por dois dias teve impacto financeiro e operacional direto. Isso levou o conselho de administração da empresa a tomar uma atitude.

Embora não houvesse sinais de exfiltração de dados confidenciais, a diretoria "não poupou esforços", como observou Arthur Brandão, para priorizar a implantação do Sophos a fim de elevar o nível de segurança para todas as empresas do grupo. Coincidentemente,o TI já tinha um planopara aumentar a segurança com a implantação do Sophos, portanto, tornou-se uma questão de simplesmente colocar o plano em ação o quanto antes.

Como a Sophos corrige uma situação de ataque e como ela será usada daqui para frente?

Para restaurar o ambiente, a equipe de TI trabalhou em colaboração com a SECUREWAY, empresa de tecnologia sediada em São Paulo, para implementar o Sophos. Eles foram capazes de investigar e mapear a origem do ataque de ransomware, proteger o ambiente de novas infecções e restaurar e reinstalar o equipamento infectado anteriormente.

"Durante o processo de resposta a incidentes, o Sophos Threat Analysis Center foi um recurso essencial", disse Arthur Brandão, explicando que permitiu identificar e bloquear ameaças no ambiente rapidamente. Com a ajuda da SECUREWAY, Arthur Brandão e sua equipe instalaram o Sophos Intercept X Advanced com XDR, que ele descreve como "essencial para identificação e correção de ameaças", em 2.550 dispositivos de computação e 200 servidores. O Sophos Intercept X combina aprendizado profundo anti-exploit, anti-ransomware e baseado em inteligência artificial (IA) para impedir ataques antes que eles afetem os sistemas. Ao integrar o aprendizado profundo, uma forma avançada de "machine learning", a segurança se torna preditiva em vez de reativa, o que é útil contra ameaças não conhecidas.

Para se defender contra os ataques de ransomware de hoje, que geralmente combinam várias técnicas avançadas com hacking em tempo real, o Sophos Intercept X usa uma abordagem abrangente para proteção de endpoint, em vez de confiar em qualquer técnica de segurança.

Agora, Arthur Brandão e toda a equipe ficam mais tranquilos ao saber que o Sophos Intercept X está prevenindo ataques de ransomware de forma preditiva, com a capacidade de reverter a criptografia não autorizada de arquivos em segundos e responder automaticamente a ameaças. O recurso XDR sincroniza endpoint nativo, servidor, firewall, e-mail, nuvem e segurança do Microsoft Office 365 para fornecer uma visão holística do ambiente de uma organização.

Com o Sophos Email Advanced e o Sophos Encryption, Arthur Brandão e sua equipe de TI podem criar políticas DLP com várias regras para grupos e usuários para garantir a proteção de informações confidenciais e selecionar opções de criptografia personalizáveis e adicionar assinaturas digitais. O console de gerenciamento Sophos Central permite o compartilhamento em tempo real de dados de segurança entre os produtos para insights mais ricos e seu abrangente painel central intuitivo baseado em nuvem alivia o fardo da equipe, liberando-os para outros projetos importantes.

Arthur Brandão afirma que, graças à Sophos, o Valgroup tem agora "maior controle e segurança do ambiente".

SOPHOS

2024-02-05 CCS-PT (NP)